



Прайс-лист на стандартні ключі безпеки YubiKey 5, YubiKey FIPS та YubiHSM2 від Вересня 2020р.

| | YubiKey 5 NFC | YubiKey 5C NFC | YubiKey 5 Nano | YubiKey 5C | YubiKey 5C Nano | YubiKey 5 CI | Security Key | Security Key NFC |
|----------------------------------|---|----------------------|----------------------|------------------------|--------------------|------------------------|---|---|
| В оптовій упаковці (по 50шт) | | | | | | | | |
| Індивідуальна упаковка | | | | | | | | |
| Ціна | грн 1800,00 | грн 2200,00 | грн 1950,00 | грн 1950,00 | грн 2350,00 | грн 2700,00 | грн 1000,00 | грн 1200,00 |
| Опис | USB-ключ автентифікації, криптостійкий, підтримує стандарти FIDO2 та U2F, безпарольний вхід, одноразові паролі OTP, статичні паролі, режим смарт-карти PIV, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP. Підтримка NFC у моделі YubiKey 5 NFC та YubiKey 5C NFC. | | | | | | USB-Ключ автентифікації, працює з будь-яким онлайн-сервісом з підтримкою FIDO2 або U2F. | USB/NFC-ключ автентифікації, працює з будь-яким онлайн-сервісом з підтримкою FIDO2 або U2F. |
| Розмір та вага | 18 x 45 x 3.3мм, 3г. | 18 x 45 x 3.3мм, 3г. | 12 x 13 x 3.1мм, 1г. | 12.5 x 29.5 x 5мм, 2г. | 12 x 10.1 x 7, 1г. | 12 x 40.3 x 5мм, 2.9г. | 18 x 45 x 3.3мм, 3г. | 18 x 45 x 3.3мм, 3г. |
| Сертифікація | | | | | | | | |
| Сертифікація FIDO certification™ | Y | Y | Y | Y | Y | Y | Y | Y |
| Сертифікація FIPS 140 | | | | | | | | |
| Підтримувані підключення | | | | | | | | |
| USB-A | Y | | Y | | | | Y | Y |
| USB-C | | Y | | Y | Y | Y | | |
| Lightning | | | | | | Y | | |
| NFC (Зв'язок на малих відстанях) | Y | Y | | | | | | Y |
| Тип пристрою | | | | | | | | |
| Клавіатура HID | Y | Y | Y | Y | Y | Y | | |
| Смарт-карта CCID | Y | Y | Y | Y | Y | Y | | |
| Пристрій FIDO HID | Y | Y | Y | Y | Y | Y | Y | Y |
| Специфікації криптографії | | | | | | | | |
| RSA 2048 | Y | Y | Y | Y | Y | Y | | |
| RSA 4096 (PGP) | Y | Y | Y | Y | Y | Y | | |
| ECC p256 | ** | ** | ** | ** | ** | ** | ** | ** |
| ECC p384 | *** | *** | *** | *** | *** | *** | | |







** ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP. Типом ключа, що генерується для ключової пари U2F, є ECC p256.

*** ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP

OATH-TOTP вимагає додатковий додаток - Yubico Authenticator; Для ключів типу YubiKey 5 NFC, сертифікація FIDO застосовується для обох видів підключення - USB і NFC.



Прайс-лист на сертифіковані ключі безпеки YubiKey FIPS від Вересня 2020р.

| | YubiKey FIPS | YubiKey Nano FIPS | YubiKey C FIPS | YubiKey C Nano FIPS |
|---|--|---|---|---|
| Моделі |  |  |  |  |
| Ціна | грн 1900,00 | грн 2200,00 | грн 2200,00 | грн 2650,00 |
| Опис | FIPS 140-2 сертифікований USB-ключ автентифікації, криптостійкий, підтримує стандарти FIDO2 та U2F, безпарольний вхід, одноразові паролі OTP, статичні паролі, режим смарт-карти PIV, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP. | | | |
| Розмір та вага | 18 x 45 x 3.3мм, 3г | 12 x 13 x 3.1мм, 1г | 12.5 x 29.5 x 5мм, 2г | 12 x 10.1 x 7, 1г |
| Сертифікація | | | | |
| Сертифікація FIDO Certification™ | Y | Y | Y | Y |
| Сертифікація FIPS 140 | Y | Y | Y | Y |
| Підтримувані підключення | | | | |
| USB-A  | Y | Y | | |
| USB-C  | | | Y | Y |
| NFC (Зв'язок на малих відстанях) | | | | |
| Тип пристрою | | | | |
| Клавіатура HID | Y | Y | Y | Y |
| Смарт-карта CCID | Y | Y | Y | Y |
| Пристрій FIDO HID | Y | Y | Y | Y |
| Специфікації криптографії | | | | |
| RSA 2048 | Y | Y | Y | Y |
| RSA 4096 (PGP) | Y | Y | Y | Y |
| ECC p256 | ** | ** | ** | ** |
| ECC p384 | *** | *** | *** | *** |

** ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP. Типом ключа, що генерується для ключової пари U2F, є ECC p256..

*** ECC застосовується тільки до аплету смарт карти; не застосовується до аплету OpenPGP.




NIST | Національний Інститут Стандартів та Технологій (США)
Сертифікація криптографічних модулів YubiKey





Апаратний модуль безпеки YubiHSM 2 для захисту криптографічних ключів на серверах

| YubiHSM 2 | |
|--|---|
| Модель |  |
| Ціна | грн 25000.00 |
| Розмір та вага | 12 мм x 13 мм x 3.1 мм, 1 грам |
| Підтримка ОС | |
| Версія | Linux CentOS 6, CentOS 7, Debian 8, Debian 9, Fedora 25, Ubuntu 1404, Ubuntu 1604 |
| | MS Windows Windows 10, Windows Server 2012, Windows Server 2016 |
| | Mac OS 10.12 Sierra, 10.13 High Sierra |
| Архітектура | amd64 |
| Криптографічні можливості | |
| Хешування | Застосовується з HMAC та асиметричними підписами <input type="checkbox"/> SHA-1, SHA-256, SHA-384, SHA-512 |
| RSA | <input type="checkbox"/> 2048, 3072, и 4096-бітні ключі <input type="checkbox"/> Підпис за допомогою PKCS#1v1.5 та <input type="checkbox"/> PSS Дешифрація PKCS#1v1.5 и OAEP |
| Еліптична криптографія (ECC) | <input type="checkbox"/> Криві: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 <input type="checkbox"/> Підпис: ECDSA (все окрім curve25519), EdDSA (тільки curve25519) Дешифрація: <input type="checkbox"/> ECDH (все окрім curve25519) |
| Упаковка ключів | Імпорт та експорт за допомогою NIST AES-CCM Wrap при 128, 196, та 256 бітах |
| Випадкові числа | Вбудований в чіп генератор реальних випадкових чисел (TRNG) з зерном NIST SP 800-90 AES 256 CTR_DRBG |
| Атестация | Згенеровані на пристрої асиметричні ключові пари можуть проходити перевірку за допомогою заводського сертифікованого ключа атестації та сертифіката, або за допомогою Вашого особистого ключа, імпортованого в модуль безпеки |
| Швидкодія | Швидкодія залежить від цільового застосування. У прикладі приведена метрика YubiHSM2, незадіяного в інших процесах: <input type="checkbox"/> RSA-2048-PKCS1-SHA256: ~139ms серед. <input type="checkbox"/> RSA-3072-PKCS1-SHA384: ~504ms серед. <input type="checkbox"/> RSA-4096-PKCS1-SHA512: ~852ms серед. <input type="checkbox"/> ECDSA-P256-SHA256: ~73ms серед. <input type="checkbox"/> ECDSA-P384-SHA384: ~120ms серед. <input type="checkbox"/> ECDSA-P521-SHA512: ~210ms серед. <input type="checkbox"/> EdDSA-25519-32 Байт: ~105ms серед. <input type="checkbox"/> EdDSA-25519-64 Байт: ~121ms серед. <input type="checkbox"/> EdDSA-25519-128 Байт: ~137ms серед. <input type="checkbox"/> EdDSA-25519-256 Байт: ~168ms серед. <input type="checkbox"/> EdDSA-25519-512 Байт: ~229ms серед. <input type="checkbox"/> EdDSA-25519-1024 Байт: ~353ms сред. <input type="checkbox"/> AES-(128 192 256)-CCM-Wrap: ~10ms серед. <input type="checkbox"/> HMAC-SHA-(1 256): ~4ms серед. <input type="checkbox"/> HMAC-SHA-(384 512): ~243ms серед. |
| Хост-інтерфейс | (USB) 1.x Full Speed (12Mbit/s) периферійний інтерфейс. |
| Фізичні характеристики | <input type="checkbox"/> Форм-фактор: 'nano', розроблений для малогабаритних місць установки, таких як внутрішні USB порти серверів <input type="checkbox"/> З поглинанням току 20 мА серед., 30 мА макс. <input type="checkbox"/> USB-A штекер |
| Забезпечення дотримання екологічних норм | <input type="checkbox"/> FCC <input type="checkbox"/> CE <input type="checkbox"/> WEEE <input type="checkbox"/> ROHS |